Definitions

- **Personally Identifiable Information (PII)**
  - PII refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.*

***OMB Memorandum, M-07-16, 22 May 2007**

- **Privacy Impact Assessment (PIA)** is an analysis of how information is handled:
  - to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
  - to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and
  - to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.*

***Army CIO/G-6 Memo, Privacy Impact Assessment Guidance, 1**

Responsibilities

- **PRIVACY OFFICERS:**
  - A Privacy Official is appointed at Command levels throughout the Army
  - Execute the privacy program in functional areas and activities under their responsibility.
  - Ensure that Privacy Act records collected and maintained within the Command or agency are properly described in a Privacy Act system of records notice.
- Ensure:
  - No undeclared systems of records are being maintained.
  - A Privacy Act Statement is provided to individuals when information is collected that will be maintained in a system of records.
  - Each Privacy Act system of records notice within their purview is reviewed biennially.
  - Updated or new System of Records Notices are submitted to the Army Privacy Office

Responsibilities

- **SYSTEM MANAGERS:**
  - Prepare new, amended, or altered Privacy Act system of records notices and submit to Command Privacy Office for review.
- **Ensure:**
  - Appropriate procedures and safeguards are developed, implemented, and maintained.
  - All personnel with access to each system are aware of their responsibilities for protecting personal information being collected and maintained under the Privacy Act.
  - Each Privacy Act system of records notice within their purview is reviewed biennially

Responsibilities

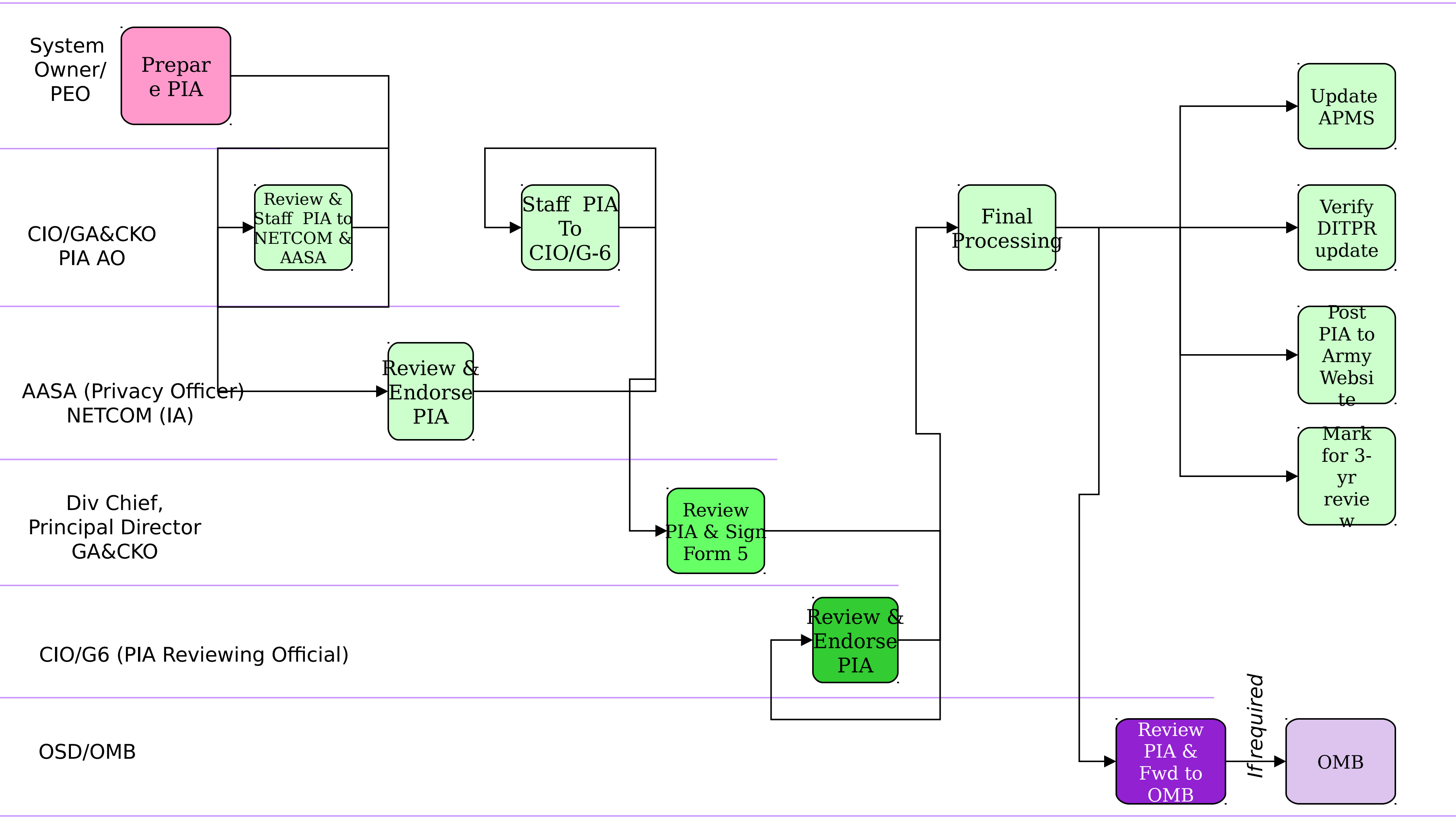
- **Information Assurance Official**
  - AR 25-2 para **5–8. Designated approving authority**

  a. The DAA is vested with the authority to formally assume responsibility for operating an IS at an acceptable level of risk. The DAA must weigh the operational need for the systems capabilities, ***the protection of personal privacy****, the protection of the information being processed, and the protection of the information environment, which includes protection of the other missions and business functions reliant on the shared information environment.*
  - Provides a unified approach to protect information stored, processed, accessed, or transmitted by Information Systems
  - Consolidates and focus' Army efforts in securing information
  - Risk management approach for implementing security safeguards

PIA Process

- Examples of completed PIA’s can be found at http://www.army.mil/ciog6/links/privacyimpact.html
- Ensure that the system’s APMS record is accurate and current
- Ensure system certification is current
- PIA preparer sign the signature sheet
- Submit PIA to CIO G-6

Army PIA Approval Process



The process is documented as if it worked properly at every step. Implied in every task is that the package may be returned to its source for correction.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

1. **Department of Defense Component.**

Entry should always begin with U. S. Army, then add the name of the system
owner's organization. Don't go into too much detail, because your audience is
the general public and they may not recognize the finer details of Army
Organization. It is very important to identify the system correctly. This is why we
ask for so many different identifiers.

2. **Name of Information Technology System.**

Enter the full name of the system, with acronym in parentheses, follow APMS name.

3. **Budget System Identification Number (SNAP-IT Initiative Number)**

If you don't know the BIN number, or can't find it in APMS, a PM or finance officer
should be able to help.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

4**. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):**

Should find this in APMS. Budget System Identification Number is a 4 digit number located in the DITPR database or IT_Registry.

5. **IT Investment (OMB Circular A-11) Unique Identifier (from IT-43/FOIT Database -- if applicable):**

Not all systems have this identifier. See Army UPI List. If your

system has a UPI, enter the number as the answer to this question. Otherwise enter N/A. For most systems the answer will be N/A

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

6. Privacy Act System of Records Notice Identifier:

If this is a Privacy Act System of Records (i.e. information is retrieved by personal identifiers specific to an individual such as name, SSN, or other unique designator)

consult the listing of System of Records Notices at

http://www.defenselink.mil/privacy/notices/

to determine the notice that applies. Army notices begin with AAFES or AO followed by the` prescribing regulation number and activity. EXAMPLE: **AO 600-8-14, Uniformed Services Identification Card**.

NOTE: Some Army systems operate under a DoD or Government-wide Systems Notice and those should also be reviewed if an Army notice is not apparent. If the system does not retrieve information through personal identifiers, indicate "N/A – this is not a Privacy Act System of Records."

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

7. OMB Information Collection Requirement Number and Expiration Date:

If your system collects PII using an OMB-approved form, the form will have an identifying number in the upper right corner of the form. (For an example, see your recent IRS form 1040). Few, if any, Army systems will use data collection forms with these numbers on them. Again, we have a list to post on the website of Army forms which contain an OMB Collection Requirement Number. If your system uses such a form, enter the number as the answer to this question. Otherwise, enter NA.

8. Type of authority to collect information (statutory or otherwise)

Indicate the statutory and/or Executive Order authority that allows the Army to collect the information and conduct this business practice. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation, use statute names or regulations in addition to citations. If this is a Privacy Act System of Records, the citations must match the authority that has been published in the Systems Notice. Also list any prescribing Army Regulations, DoD Directives or Instructions. As an example, Executive Order 9397 allows the Army to use the SSN as the primary identifier for individuals and should be listed on most systems. NOTE: The Systems Notice may require an update to include any additional authority reflected in the PIA.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup)

Identify whether this is a new IT system, an existing system with no PIA, a Significantly modified IT System, or other. Identify whether the system contains information on members of the public (i.e. not agency employees or contractors). Part of the response to this question should address business requirements, practices and procedures that relate directly to an individual and the use(s) of their PII. A generic technical description of the system often does not provide enough information to evaluate the PIA. Be sure to describe: (1) The system purpose; (2) A description of a primary transaction conducted on or by the system; (3) A general overview of the modules and subsystems, and their functions.____________

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

10. **Identifiable Information to be Collected, its Nature and Source.**

List all data elements in the system linked to an individual in detail. This must include all data elements listed in the System of Records Notice under the section “Categories of records in the system”. Also indicate the source, who or what is providing the information, where this information will be provided from, (e.g., the individual, existing DoD IT system (specify), other Federal database (specify), etc). It is suggested the table of data elements in the system be reviewed to ensure complete PII is described. NOTE: The Systems Notice may require an update to include any additional PII reflected in the PIA.

(1) Examples of PII: Name Other Names Used, Social Security Number, Truncated SSN, Drivers License, Other ID Number, Citizenship Legal Status, Gender Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Telephone Home Telephone Numbers, Personal Email Address Mailing/Home Address, Religious Preference, Security Clearance, Mother's Maiden Name, Mother's Middle Name, Spouse Information, Marital Status, Biometrics, Child Information, Vehicle Identifiers, Medical Data Disability Information, Financial Information Employment Information, Military Records, Law Enforcement Data, Emergency Contact, Education Information

(*Electronic Data Interchange Personal Identifier (DEERS Record Locator)

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

11. Method of Information Collection.

Indicate how the information will be collected. Methods that may apply are: Paper Form, Face to Face Contact, Telephone Interview, Fax, Email, Web, Information Sharing from System to System, Others.

Example: Personal information is provided by the individual record subject through completion of forms and via personal interview. Some information (Specify) is acquired from other Army/DoD personnel database systems (Specify).

12. Purpose of Collection and How Identifiable Information/Data will be used.

Describe why you are collecting the PII and state the intended use (e.g. Verification, Identification, Authentication, Data Matching; along with description of Intended Use - e.g., Mission related use (define), Administrative use (define). This should include a description from an individual record subject’s standpoint. State the Army requirements and business practices to be accomplished.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

13. Does system create new data about individuals

through aggregation?

Will data from two or more systems be combined to derive new data or

Create previously unavailable data about an individual. In most cases the

answer to this question is “No”. If “Yes”, describe what data elements from

which systems are combined and describe the new data that is developed.

.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

14. Internal and External Information/Data Sharing

List all Army activities followed by all other (DoD, Federal/State/Local/Foreign government, private organizations, etc.) that receive information or data from the system. NOTE: If this is a Privacy Act System of Records, disclosures outside DoD must include those published under the System of Records Notice under the section “Routine Uses”. Agencies identified Under Internal and External Information/Data Sharing should be accompanied by a brief description of the purpose for disclosing the information to the agency. NOTE: The Systems Notice may require an update to include any additional external data sharing outside DoD reflected in the PIA. Please ensure that all sharing within the Army; with other DoD components; with other Federal Agencies; with State and Local Agencies; with Contractors (specify contractor’s name and describe the language in the contract that safeguards PII); and other (e.g., colleges) are specified. As a standard entry, we are using the following for all systems: “Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.”

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

15. Opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted.

This response should describe Privacy Act Statements provided to individuals on forms (hardcopy or electronic) on system applications or on websites.

Example: See attached Privacy Act Statement.

16. Information Provided to the Individual, the Format, and the Means of Delivery.

This response is similar to Item 15 and should describe that Privacy Advisory Statements are provided to individuals as information is collected.

Example: See attached Privacy Advisory Statement.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

17. Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

Indicate in great detail all physical, business and automation safeguards in place to ensure the data is protected from unauthorized access. Also indicate the authorized users of the system.

Identify:

- Who will have access to PII system- Users, Developers, System Administrators, Contractors or any others
- Type of Physical Controls-Security Guards, Cipher Locks, Identification Badges, Biometrics, Key Cards
- Technical Controls-User ID, Biometrics, Password, Firewall, Intrusion Detection System, Encryption, DoD PKI Cert
- Administrative Controls-Perform periodic security audits (frequency), monitoring of user’s security practices, limited access of users to equipment and information
- Has your system undergone a certification and accreditation process and if so, what is the current status? ATO-Authorization to Operate; IATO-Interim ATO; IATT-Interim Authorization to test; DATO- Denial of Auth to Operate; None-Not yet Accredited; Not Required

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

18. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures.

If there are issues with safeguarding the data, they should be outlined here. For most systems it would most likely be correct to state that appropriate safeguards are in place for the collection, use, and sharing of information. Also indicate the problems (if any) that might arise if individuals are afforded an opportunity to object to the collection of information. An example might be advising a person that we are collecting information when conducting an undercover criminal investigation. For most instances, we should model after the Privacy Act Advisory Statement. Example: Individuals who object to providing required information may be unable to enter the Armed Forces. In most cases we should also state if appropriate that security measures are adequate and risk is minimal. Information is protected by user passwords, firewalls, antivirus software, CAC access, and data-at-rest protection software on portable laptops. **Example:** Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing the individual the opportunity to object or consent.

EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

19. Classification and Publication of Privacy Impact Assessment.

Indicate the classification of the system and whether the Privacy Impact Assessment may be published in its entirety, or identify specific portions not recommended for publication. In most cases, it is appropriate to indicate:

Example: The data in the system is For Official Use Only. The PIA may be published in full.